Semester II Examinations 2012/ 2013

Exam Code(s)	4IF1
Exam(s)	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	
Repeat Paper	No
Discipline(s)	Information Technology
Course Co-ordinator(s)	
Internal Examiner(s)	Professor G Lyons Dr. M Madden Dr. C Mulvihill*
External Examiner(s)	Professor M. O'Boyle
No. of Pages	3
Duration	**3 hours**
Instructions:	Attempt any four questions. All questions will be marked equally.

Requirements:
MCQ
Handout
Statistical/ Log Tables
Cambridge Tables
Graph Paper
Log Graph Paper
Other Materials

Release to Library: Yes

PTO

1

(a) Develop an intuitive explanation of the mathematics that underlies RSA, touching on the Euler-Fermat theorem in the course of your answer. (8 marks)

(b) 'So–called *probabilistic encryption*, such as is found in ElGamal (key elements) and in RSA-OAEP (padding) can make an exhaustive plaintext attack difficult'. By considering a domain containing only limited plaintexts, outline why such an attack is less likely to succeed if such encryption is employed. (6 marks)

(c) Alice encrypts an assignment with Bob's public encryption key. She then signs the encrypted assignment with her private signature key. Both the encrypted assignment and the signature are then sent to Bob in a message. This is intercepted. An attacker replaces Alice's signature with his and then forwards the message to Bob. Is this possible in your view and, if so, advise Alice on how to deal with this scenario. (6 marks)

2

(a) Give your understanding of the term 'Feistel Cipher'. (6 marks)

(b) A block cipher can be operated in so-called *electronic codebook* mode. Discuss any one attack against this mode of operation, suggesting when it might be useful. (6 marks)

(c) 'In so-called *cipher feedback* mode, decryption of a block cipher takes place using the encryption algorithm of the block cipher' Explain why this is so. (8 marks)

3

(a) Consider a new electronic commerce application implementing a *first-price sealed bid* auction, where each party submit exactly one secret bid and the highest one wins. In the application, parties in fact submit a hash of their bid as a commitment. After the competition closes, they are required to reveal their actual bids. Suppose that there are exactly two bidders, Alice and Bob. Show how knowledge of a hashing collision could give Bob an advantage if Alice reveals her bid first. (8 marks)

(b) 'To achieve non-repudiation with symmetric keys in the context of message authentication codes a trusted third party should be employed'. Sketch how this might work. (6 marks)

(c) In the context of low-level penetration tests of a company, explain what is meant by the term 'ARP cache poisoning' and list one way it could be used as an attack and one way to prevent it. (6 marks)

PTO

4

(a) In connection with FIPS PUB 140-2, security requirements for cryptographic modules, distinguish briefly between non-deterministic and deterministic random number generators. Why in your view are there no FIPS approved non-deterministic random number generators? (8 marks)

(b) Freshness in a communication is generally provided by clock, sequence number, or nonce mechanisms. Explain any one of these three schemes. (6 marks)

(c) Give a brief account of zero-knowledge entity authentication using any example of your own devising to illustrate the relevant probabilities. Explain the term 'independent event' in the course of your answer. (6 marks)

5

(a) Give your understanding of the three terms confidentiality, integrity and availability in the context of computer security. (6 marks)

(b) What type of access environment might be expected to enforce 'no read up' (the ss-property) and 'no write down' (the *-property) between subjects and objects? Explain what is meant by 'no read up' and 'no write down' in the course of your answer. (6 marks)

(c) The hospital is considering installing and customising a computer system for patient records. They have identified integrity of data as the single most important issue for their domain. Would a scheme such as that in **5 (b)** be the most suitable for their needs? If not, what would you suggest? (8 marks)

6

(a) Explain what is meant by the 'Daubert Criteria' and why they apply to computer forensics. (6 marks)

(b) You have been told that a well-known steganographic program has been downloaded by an employee in your organisation. Would you consider this worthy of investigation and, if so, how would such an investigation be likely to proceed in the light of your company's policies and procedures? (6 marks)

(c) 'Recent work by Müller and Spreitzenbarth has shown that RAM contents from smartphones can be recovered via cold boot attacks'. Discuss the implications of this statement. (8 marks)

7

'Embedded devices, logs and large-scale data mining lead to a future where there is no privacy'. Discuss this statement. (20 marks)